Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

NEW QUESTION 1
- (Exam Topic 3)
You are designing a new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.
You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

A. the Azure landing zone accelerator
B. the Azure Will-Architected Framework
C. Azure Security Benchmark v3
D. Azure Advisor

Answer: A

NEW QUESTION 2
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.
In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.
Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

NEW QUESTION 3
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions that allow traffic from the Front Door service tags. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure

NEW QUESTION 4
- (Exam Topic 3)
Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment. You need to recommend the top three modernization areas to prioritize as part of the plan.
Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. data, compliance, and governance
B. user access and productivity
C. infrastructure and development
D. modern security operations
E. operational technology (OT) and IoT

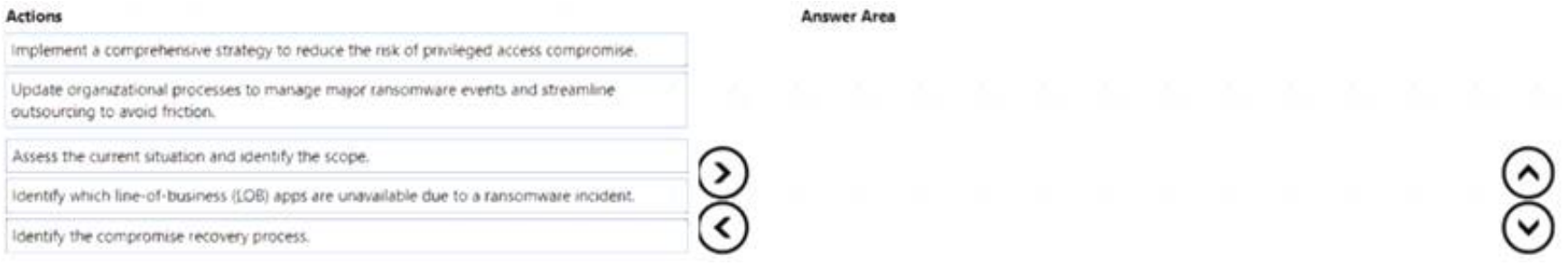
Answer: ABD

NEW QUESTION 5
- (Exam Topic 3)
You have an operational model based on the Microsoft Cloud Adoption framework for Azure.
You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, database, files, and storage accounts.
What should you include in the recommendation?

A. security baselines in the Microsoft Cloud Security Benchmark
B. modern access control
C. business resilience
D. network isolation

Answer: A

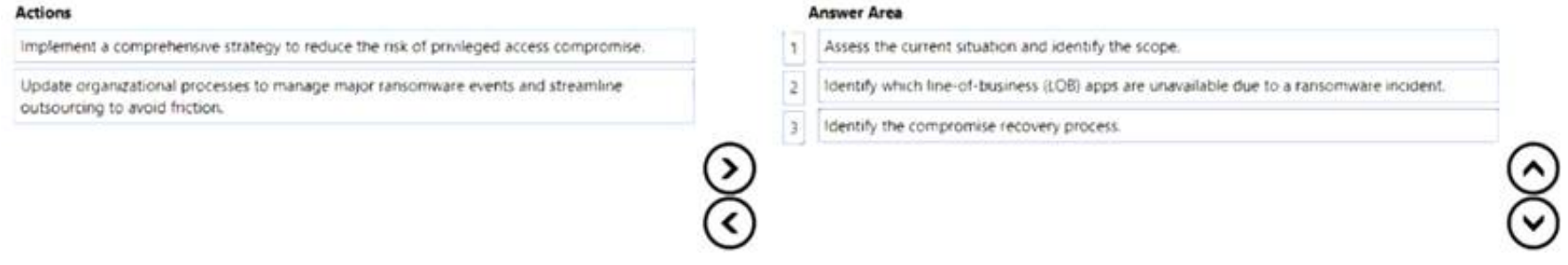
NEW QUESTION 6
- (Exam Topic 3)
Your company wants to optimize ransomware incident investigations.
You need to recommend a plan to investigate ransomware incidents based on the Microsoft Detection and Response Team (DART) approach.
Which three actions should you recommend performing in sequence in the plan? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 7
- (Exam Topic 3)
You have a Microsoft 365 subscription.
You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.
Which two services should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Cloud Apps
B. Azure AD Application Proxy
C. Azure Data Catalog
D. Azure AD Conditional Access
E. Microsoft Purview Information Protection

Answer: AD

NEW QUESTION 8
- (Exam Topic 3)
You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. AJI the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.
You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:
• A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
• A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers
What should you use for each risk? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

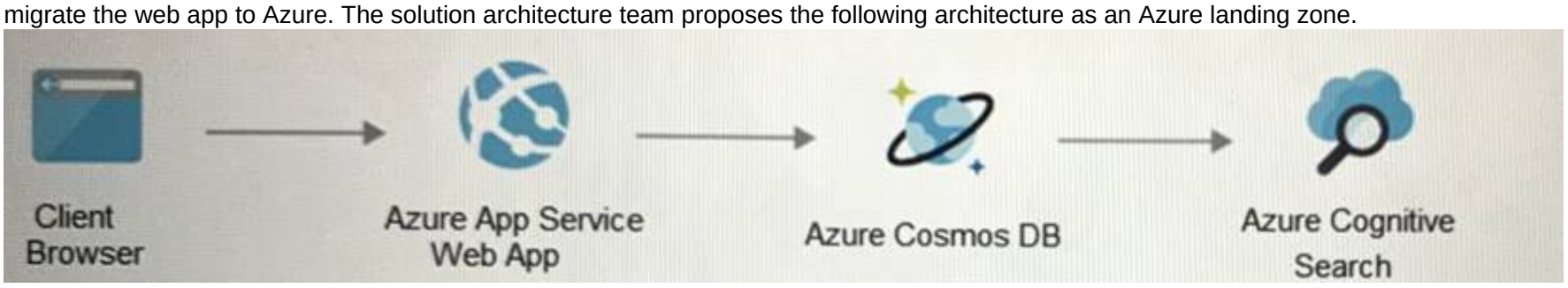
A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 9
- (Exam Topic 3)
Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



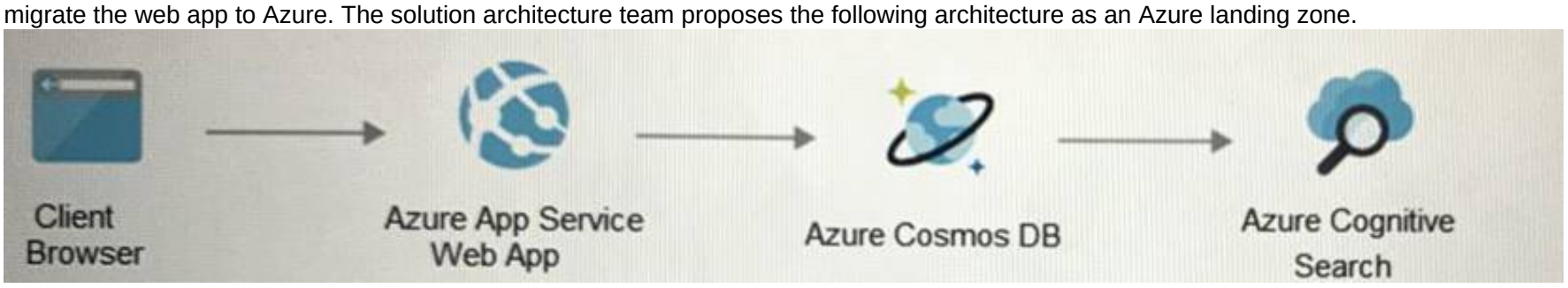
You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Key Vault to store credentials.

A. Yes
B. No

Answer: B

Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

NEW QUESTION 10
- (Exam Topic 3)
Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://www.varonis.com/blog/securing-access-azure-webapps

NEW QUESTION 10
- (Exam Topic 3)
You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers.
In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Linux containers deployed to Azure Container Registry
B. Linux containers deployed to Azure Kubernetes Service (AKS)
C. Windows containers deployed to Azure Container Registry
D. Windows containers deployed to Azure Kubernetes Service (AKS)
E. Linux containers deployed to Azure Container Instances

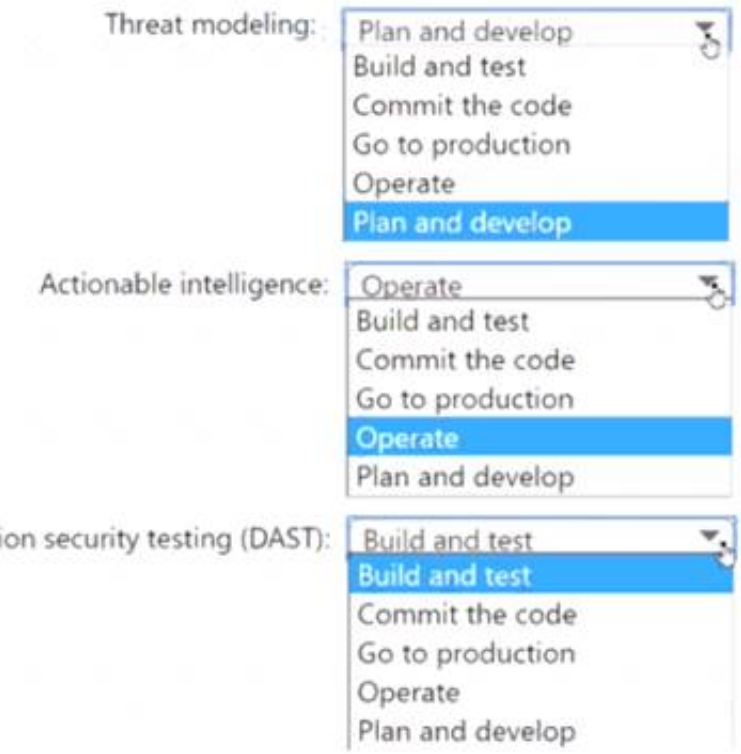
Answer: AC

Explanation:

https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-sec https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabi

NEW QUESTION 14
- (Exam Topic 3)
You need to recommend a security methodology for a DevOps development process based on the Microsoft Cloud Adoption Framework for Azure.
During which stage of a continuous integration and continuous deployment (CI/CD) DevOps process should each security-related task be performed? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point

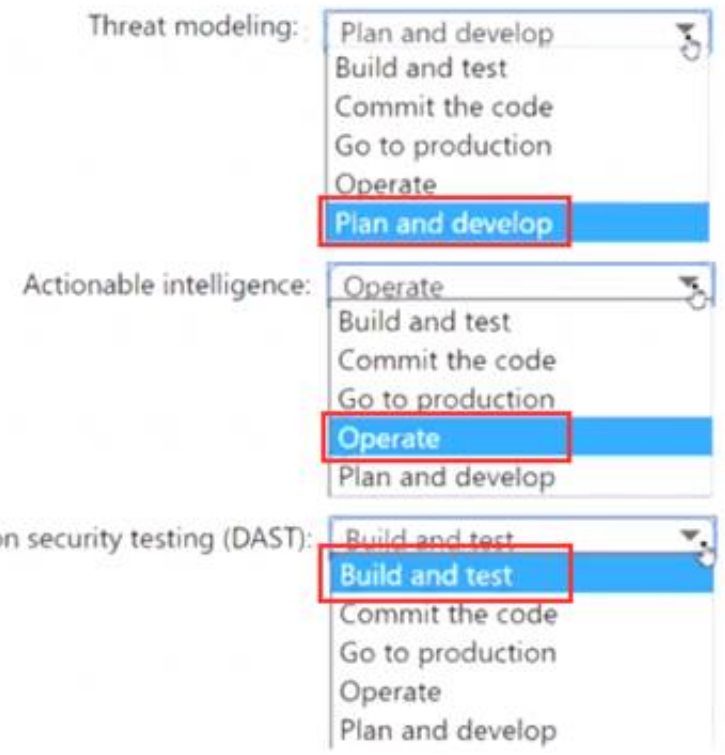
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 18
- (Exam Topic 3)
You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AO credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

A. an Azure AD enterprise application
B. a retying party trust in Active Directory Federation Services (AD FS)
C. Azure AD Application Proxy
D. Azure AD B2C

Answer: A

NEW QUESTION 23

- (Exam Topic 3)
You have a customer that has a Microsoft 365 subscription and an Azure subscription.
The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.
You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

A. Microsoft Information Protection
B. Microsoft Defender for Endpoint
C. Microsoft Sentinel
D. Microsoft Endpoint Manager

Answer: D

Explanation:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboa

NEW QUESTION 27
- (Exam Topic 3)
You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

A. Add Microsoft Sentinel data connectors.
B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
D. Obtain Azure Active Directory Premium Plan 2 licenses.

Answer: A

NEW QUESTION 29
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel deployment.
You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events. What should you recommend using in Microsoft Sentinel?

A. playbooks
B. workbooks
C. notebooks
D. threat intelligence

Answer: B

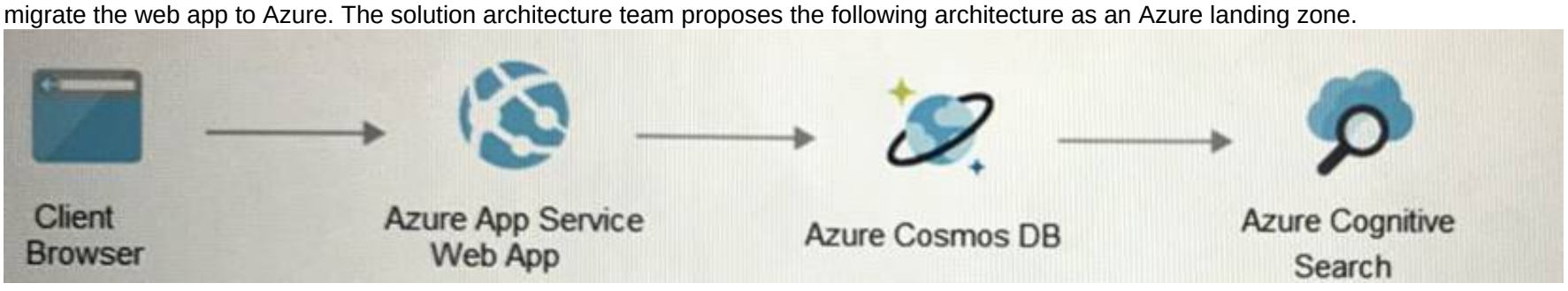
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

NEW QUESTION 31
- (Exam Topic 3)
A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.
All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.
The customer plans to deploy Microsoft Sentinel.
You need to recommend configurations to meet the following requirements:
• Ensure that the security operations team can access the security logs and the operation logs.
• Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.
Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
B. Use the Azure Monitor agent with the multi-homing configuration.
C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
D. Create a custom collector that uses the Log Analytics agent.

Answer: BC

NEW QUESTION 34
- (Exam Topic 3)
Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.
Solution: You recommend creating private endpoints for the web app and the database layer. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.
https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints

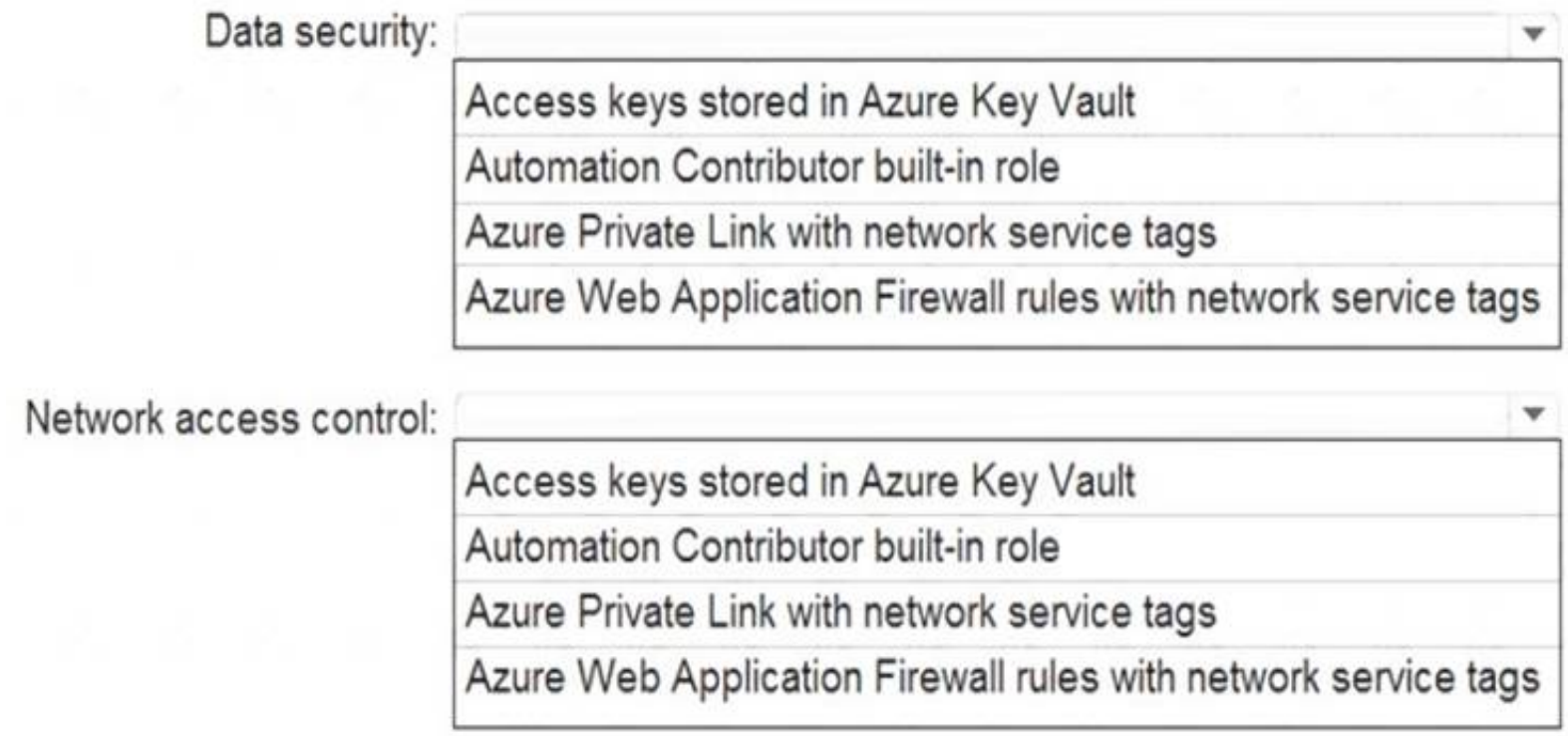
NEW QUESTION 39
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. Azure Active Directory (Azure AD) Conditional Access App Control policies
B. OAuth app policies in Microsoft Defender for Cloud Apps
C. app protection policies in Microsoft Endpoint Manager
D. application control policies in Microsoft Defender for Endpoint

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/sele

NEW QUESTION 44
- (Exam Topic 3)
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.
You need to recommend a solution to secure the components of the copy process.
What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



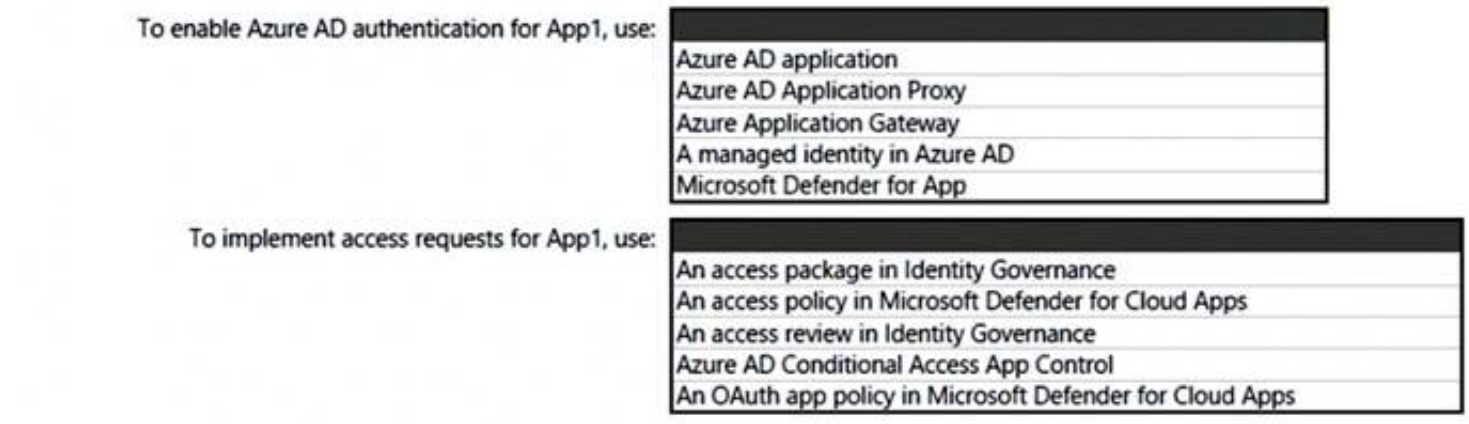
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Data Security = Access Keys stored in Azure Key Vault
Network access control = Azure Private Link with network service tags
https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security

NEW QUESTION 46
- (Exam Topic 3)
You are creating the security recommendations for an Azure App Service web app named App1. App1 has the following specifications:
• Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
• Users will authenticate by using Azure Active Directory (Azure AD) user accounts. You need to recommend an access security architecture for App1.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1 is the Azure AD Application
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
Box 2 is Access Package in Identity Governance
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cr

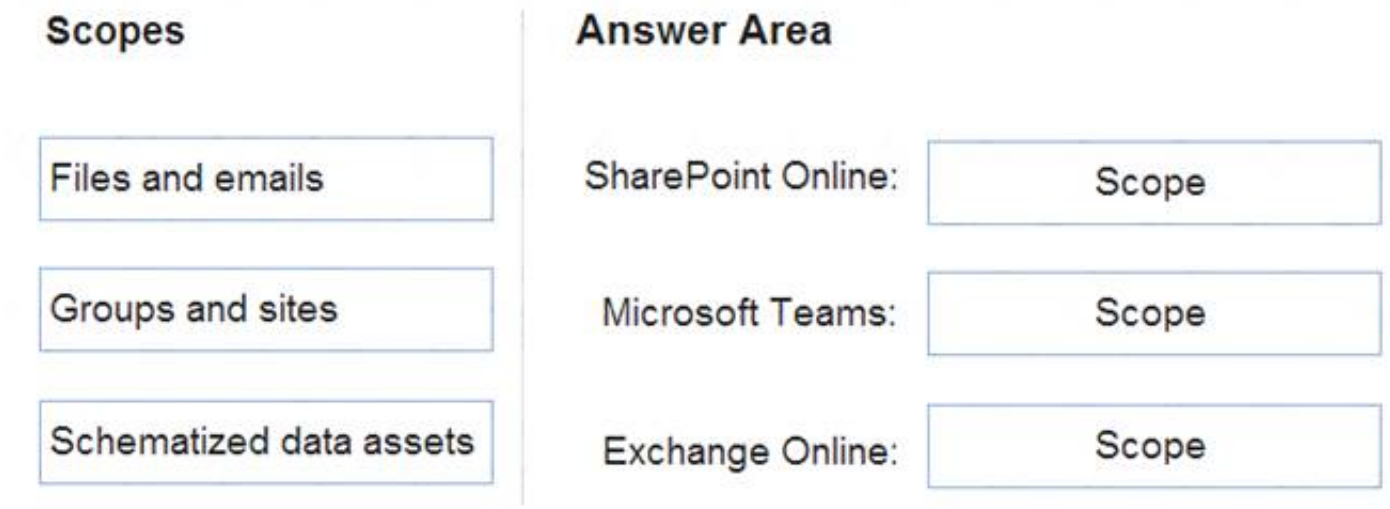
NEW QUESTION 50
- (Exam Topic 3)
Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices.
You plan to use security baselines from the Microsoft Security Compliance Toolkit.
What should you recommend using to compare the baselines to the current device configurations?

A. Microsoft Intune
B. Policy Analyzer
C. Local Group Policy Object (LGPO)
D. Windows Autopilot

Answer: B

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework

NEW QUESTION 53
- (Exam Topic 3)
Your company has Microsoft 365 E5 licenses and Azure subscriptions.
The company plans to automatically label sensitive data stored in the following locations:
• Microsoft SharePoint Online
• Microsoft Exchange Online
• Microsoft Teams
You need to recommend a strategy to identify and protect sensitive data.
Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Groups and sites Box 2: Groups and sites Box 3: Files and emails –
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide Go to label scopes

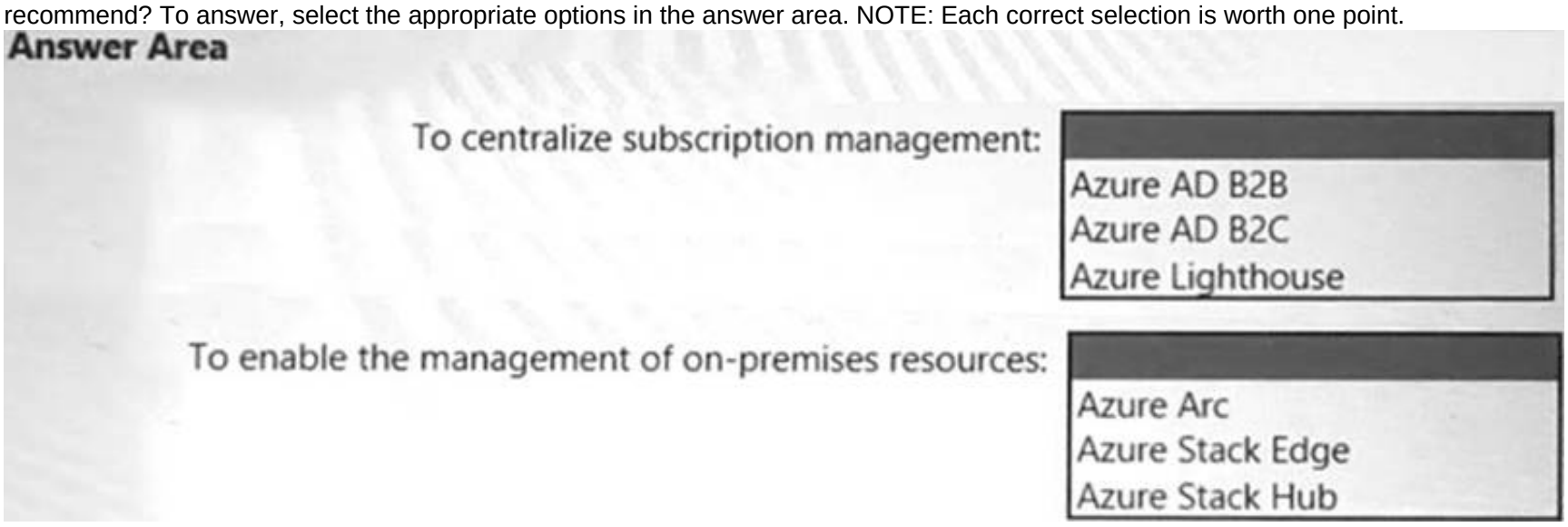
NEW QUESTION 55
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?

A. From Defender for Cloud, review the Azure security baseline for audit report.
B. From Defender for Cloud, review the secure score recommendations.
C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
D. From Defender for Cloud, enable Defender for Cloud plans.

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula

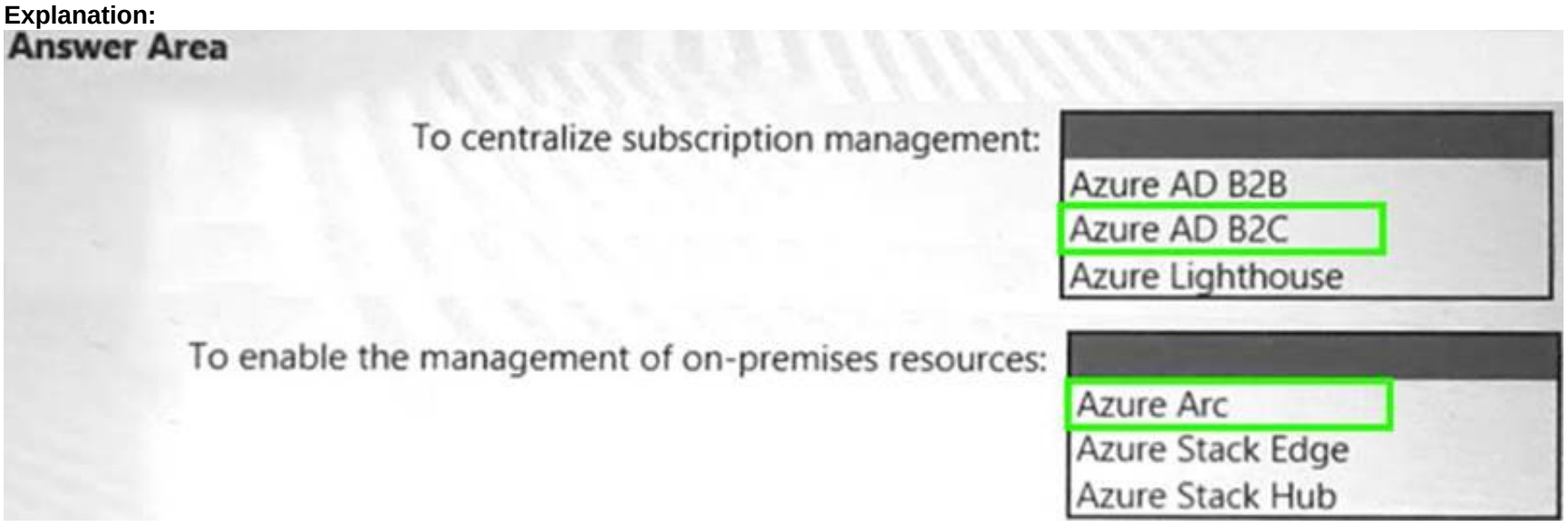
NEW QUESTION 60
- (Exam Topic 2)
You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid requirements. What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 64
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
The company plans to deploy 45 mobile self-service kiosks that will run Windows 10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:
• Ensure that only authorized applications can run on the kiosks.
• Regularly harden the kiosks against new threats.
Which two actions should you include in the recommendations? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard the kiosks to Azure Monitor.
B. Implement Privileged Access Workstation (PAW) for the kiosks.
C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

Answer: DE

Explanation:
(https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerab

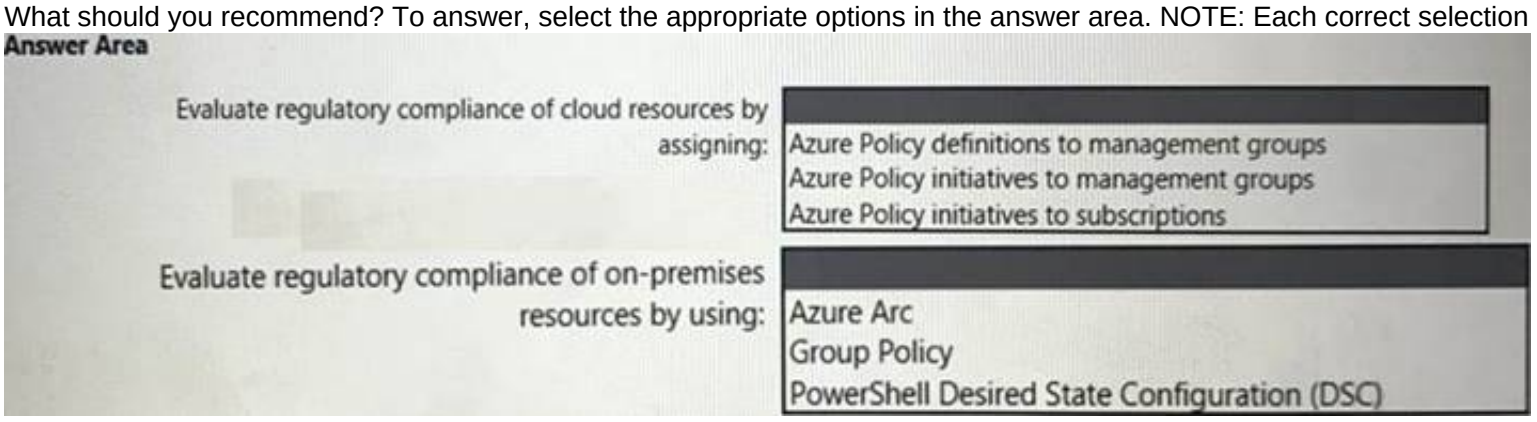
NEW QUESTION 67
- (Exam Topic 2)
To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Security Assertion Markup Language (SAML)
B. NTLMv2
C. certificate-based authentication
D. Kerberos

Answer: AD

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-o https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-w https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

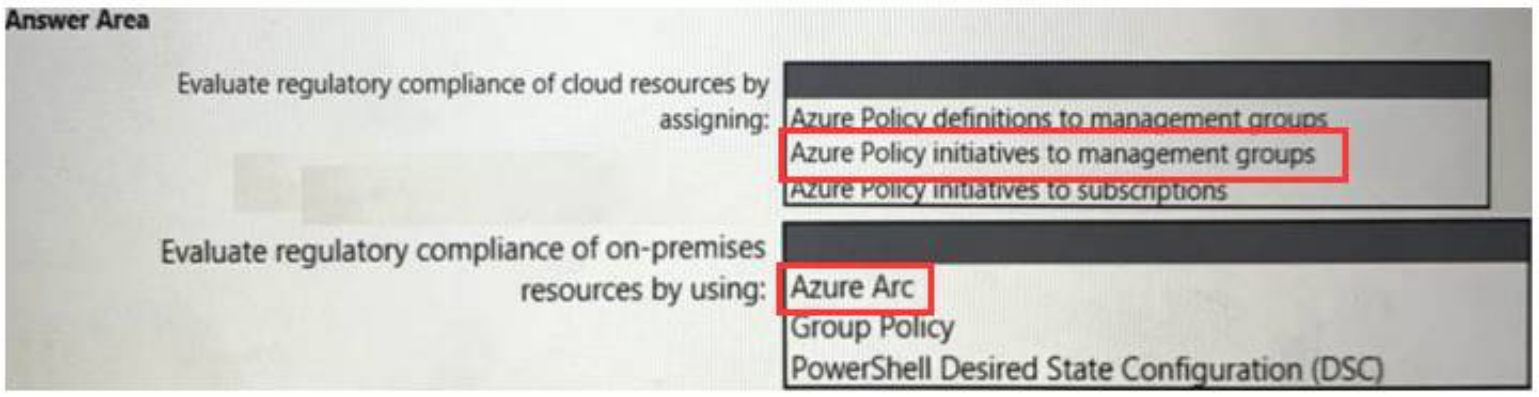
NEW QUESTION 69
- (Exam Topic 2)
You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



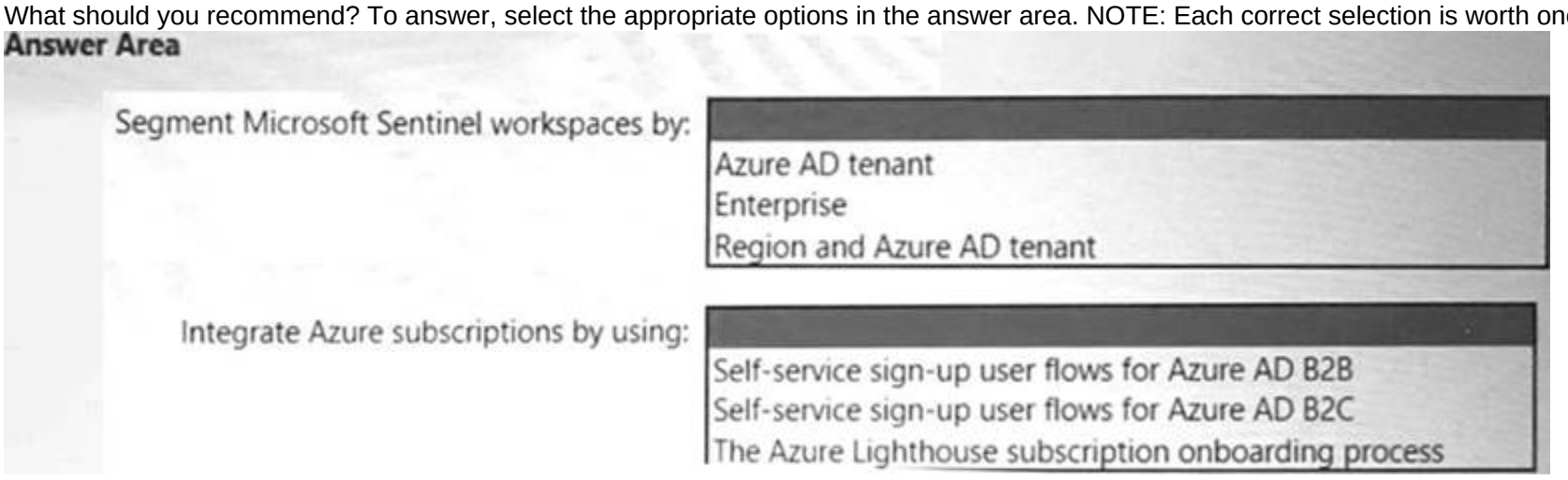
NEW QUESTION 73
- (Exam Topic 2)
You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.
What should you configure for each landing zone?

A. Azure DDoS Protection Standard
B. an Azure Private DNS zone
C. Microsoft Defender for Cloud
D. an ExpressRoute gateway

Answer: D

Explanation:
One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive. Given the landing zone requirements of
1) "Use a DNS namespace of litware.com"
2) "Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints"

NEW QUESTION 78
- (Exam Topic 2)
You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel requirements, and the regulatory compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Segment Microsoft Sentinel workspaces by: Region and Azure AD tenant Lighthouse subscription

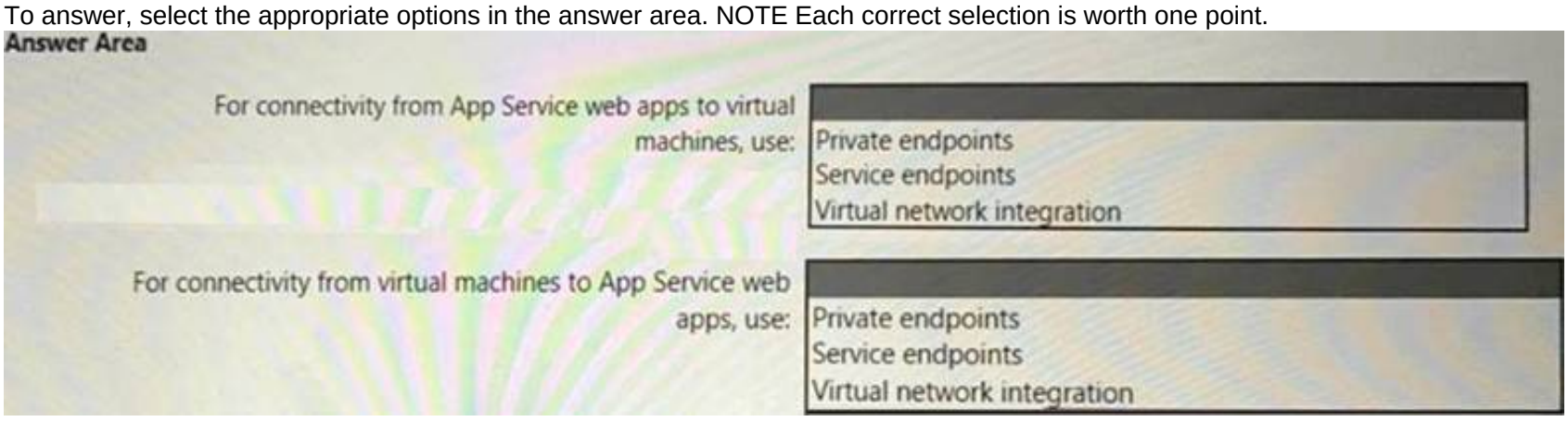
NEW QUESTION 81
- (Exam Topic 2)
You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.
Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

A. Azure AD Conditional Access
B. Microsoft Defender for Cloud Apps
C. Microsoft Defender for Cloud
D. Microsoft Defender for Endpoint
E. access reviews in Azure AD

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#c https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cl

NEW QUESTION 82
- (Exam Topic 2)
You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend?
To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Virtual Network Integration - correct
Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network.
Box 2: Private Endpoints. - correct
You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.

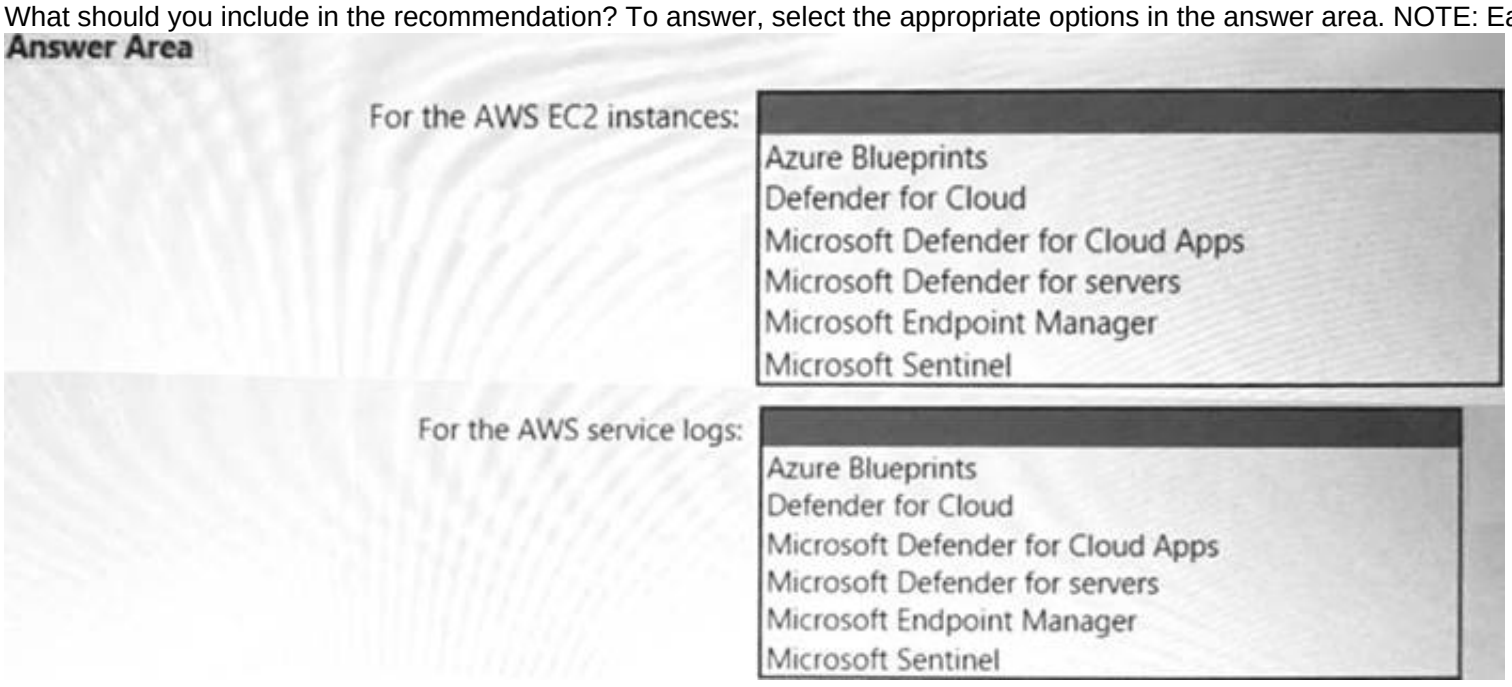
NEW QUESTION 86
- (Exam Topic 1)
You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?

A. Azure Key Vault
B. GitHub Advanced Security
C. Application Insights in Azure Monitor
D. Azure DevTest Labs

Answer: B

Explanation:
https://docs.microsoft.com/en-us/learn/modules/introduction-github-advanced-security/2-what-is-github-advanc

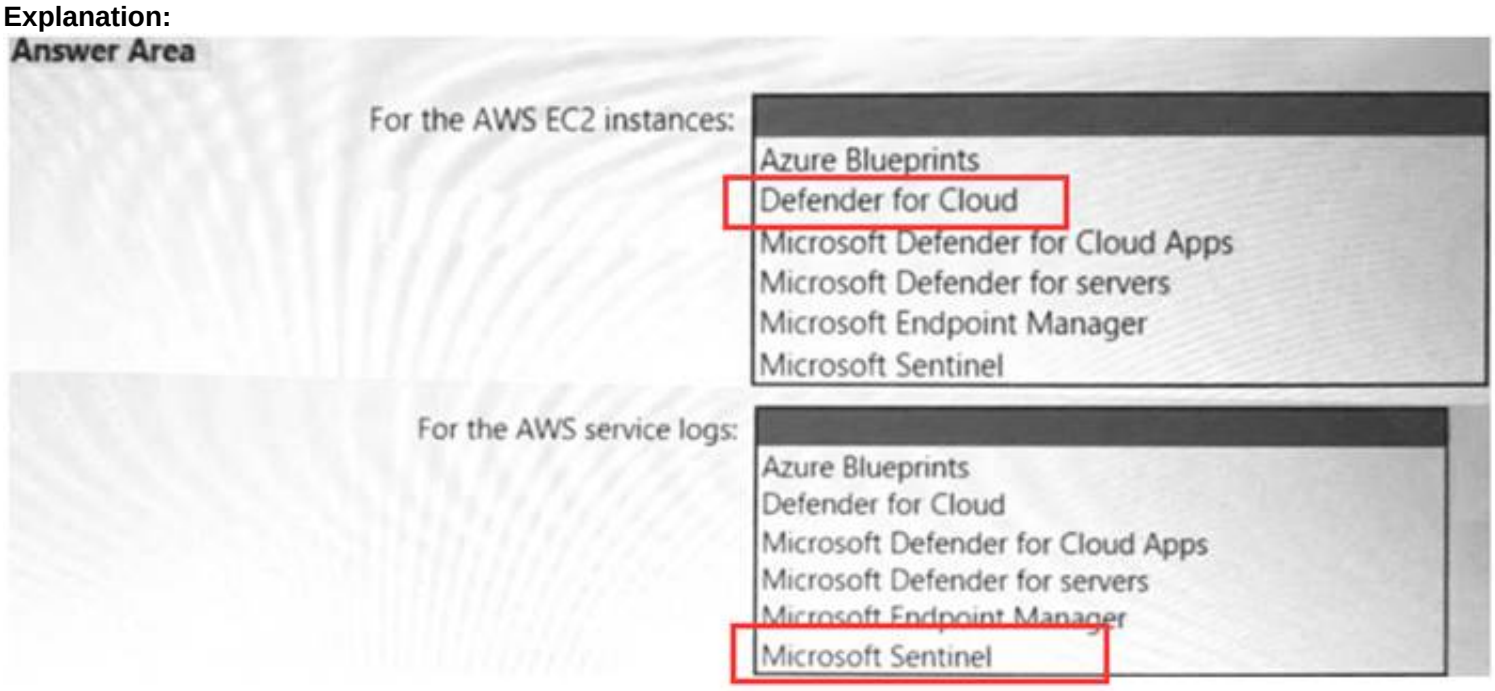
NEW QUESTION 87
- (Exam Topic 1)
You need to recommend a solution to meet the AWS requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 88
- (Exam Topic 1)
You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation? (Choose Two)

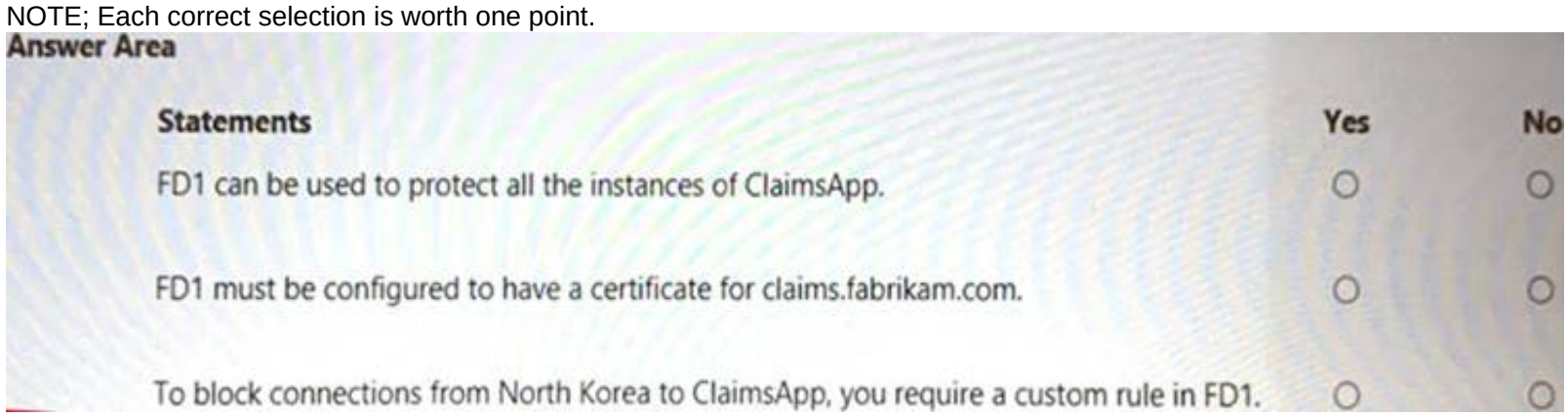
A. Onboard the virtual machines to Microsoft Defender for Endpoint.
B. Onboard the virtual machines to Azure Arc.
C. Create a device compliance policy in Microsoft Endpoint Manager.
D. Enable the Qualys scanner in Defender for Cloud.

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-

NEW QUESTION 89
- (Exam Topic 1)
You are evaluating the security of ClaimsApp.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

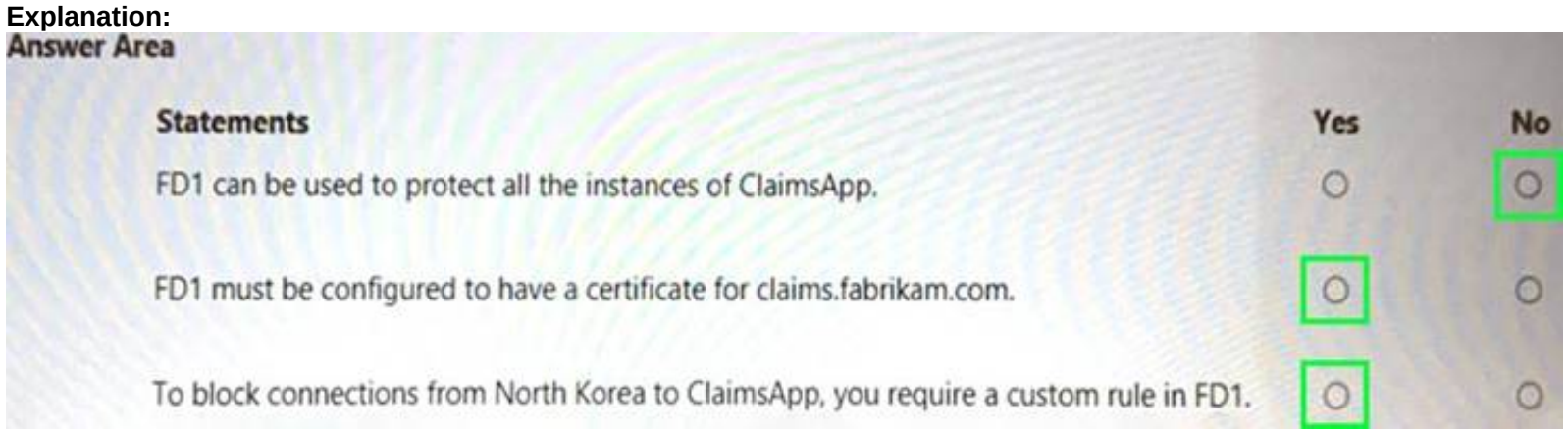
NOTE; Each correct selection is worth one point.



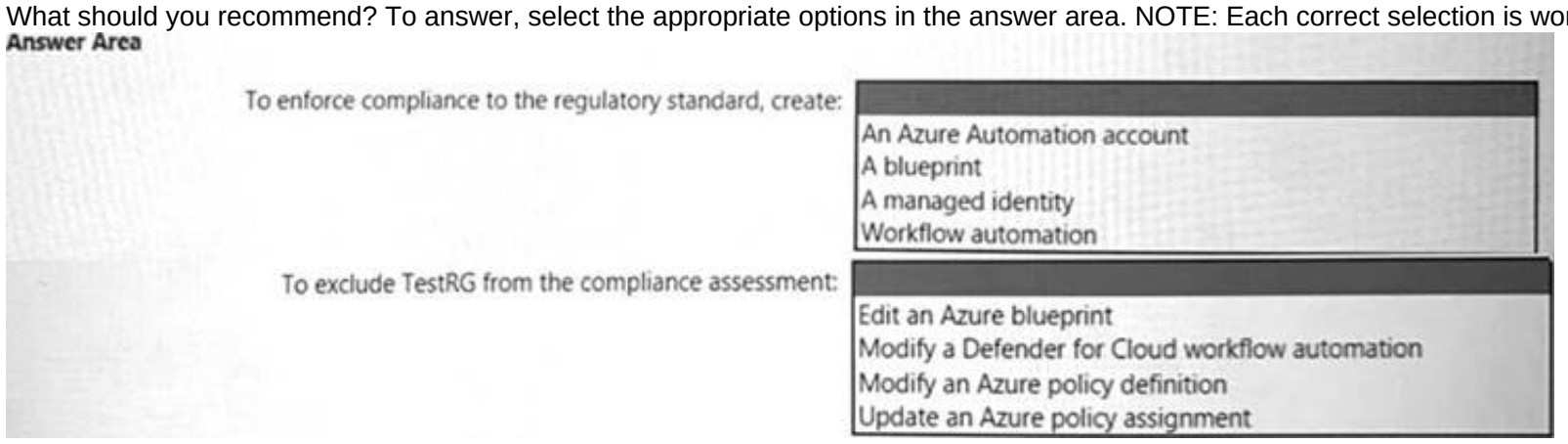
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 92
- (Exam Topic 1)
You need to recommend a solution to meet the compliance requirements.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1 = A Blueprint
Box 2 = Update an Azure Policy assignment
https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure
while it is in policy assignment
- https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure

NEW QUESTION 97
- (Exam Topic 1)
You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

A. an Azure Bastion host
B. a network security group (NSG)
C. just-in-time (JIT) VM access
D. Azure Virtual Desktop

Answer: A

Explanation:
The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image."
https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image

NEW QUESTION 98
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend configuring gateway-required virtual network integration. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure

NEW QUESTION 101
- (Exam Topic 3)
Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access integration with user flows and custom policies
B. Azure AD workbooks to monitor risk detections
C. custom resource owner password credentials (ROPC) flows in Azure AD B2C
D. access packages in Identity Governance
E. smart account lockout in Azure AD B2C

Answer: AC

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

NEW QUESTION 104
- (Exam Topic 3)
Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:
• Computers that run either Windows 10 or Windows 11
• Tablets and phones that run either Android or iOS
You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored. What should you include in the recommendation?

A. eDiscovery
B. retention policies
C. Compliance Manager
D. Microsoft Information Protection

Answer: D

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

NEW QUESTION 109
- (Exam Topic 3)
You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.
The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.
You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.
Which security control should you recommend?

A. app discovery anomaly detection policies in Microsoft Defender for Cloud Apps
B. adaptive application controls in Defender for Cloud
C. Azure Security Benchmark compliance controls m Defender for Cloud
D. app protection policies in Microsoft Endpoint Manager

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute-recommendati

NEW QUESTION 110
- (Exam Topic 3)
You have an Azure subscription.
You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar. Developers use Azure DevOps to deploy web apps to App Service Environments- When a new app is
deployed, a CNAME record for the app is registered in contoso.com.
You need to recommend a solution to secure the DNS record tor each web app. The solution must meet the following requirements:
• Ensure that when an app is deleted, the CNAME record for the app is removed also
• Minimize administrative effort.
What should you include in the recommendation?

A. Microsoft Defender for DevOps
B. Microsoft Defender foe App Service
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for DNS

Answer: C

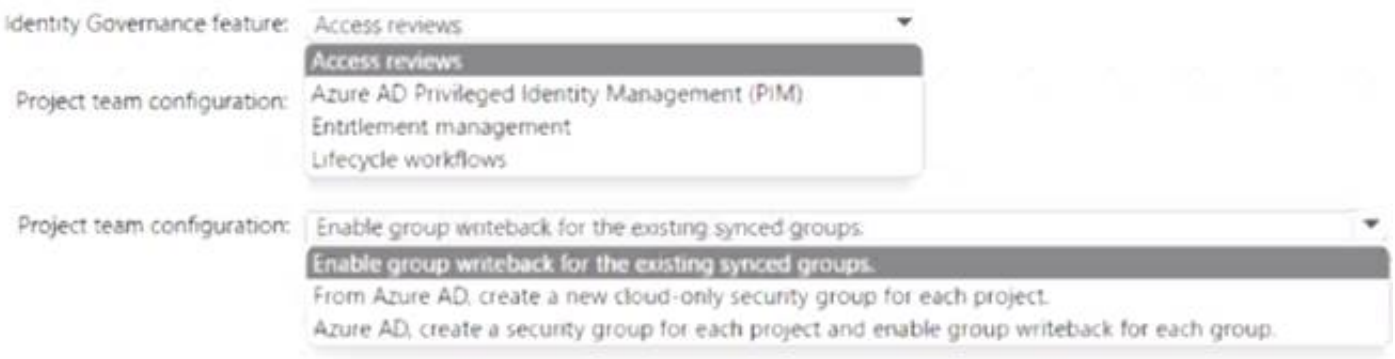
NEW QUESTION 112
- (Exam Topic 3)
You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically
What should you use?

A. the regulatory compliance dashboard in Defender for Cloud
B. Azure Policy
C. Azure Blueprints
D. Azure role-based access control (Azure RBAC)

Answer: B

Explanation:
https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-w

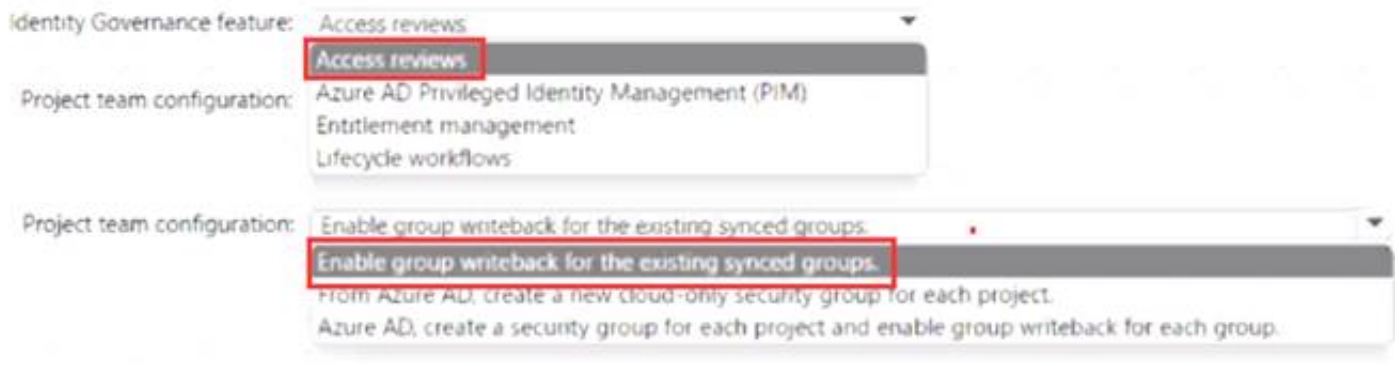
NEW QUESTION 114
- (Exam Topic 3)
Your network contains an on-premises Active Directory Domain Services (AO DS) domain. The domain contains a server that runs Windows Server and hosts shared folders The domain syncs with Azure AD by using Azure AD Connect Azure AD Connect has group writeback enabled.
You have a Microsoft 365 subscription that uses Microsoft SharePoint Online.
You have multiple project teams. Each team has an AD DS group that syncs with Azure AD Each group has permissions to a unique SharePoint Online site and a Windows Server shared folder for its project. Users routinely move between project teams.
You need to recommend an Azure AD identity Governance solution that meets the following requirements:
• Project managers must verify that their project group contains only the current members of their project team
• The members of each project team must only have access to the resources of the project to which they are assigned
• Users must be removed from a project group automatically if the project manager has MOT verified the group s membership for 30 days.
• Administrative effort must be minimized.
What should you include in the recommendation? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.
Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 117
- (Exam Topic 3)
A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.
The customer discovers that several endpoints are infected with malware. The customer suspends access attempts from the infected endpoints.
The malware is removed from the end point.
Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Defender for Endpoint reports the endpoints as compliant.

B. Microsoft Intune reports the endpoints as compliant.
C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
D. The client access tokens are refreshed.

Answer: CD

Explanation:
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

NEW QUESTION 121
- (Exam Topic 3)
Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:
• Minimizes manual intervention by security operation analysts
• Supports Waging alerts within Microsoft Teams channels What should you include in the strategy?

A. data connectors
B. playbooks
C. workbooks
D. KQL

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

NEW QUESTION 123
- (Exam Topic 3)
You are designing the encryption standards for data at rest for an Azure resource
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

NEW QUESTION 126
- (Exam Topic 3)
Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices.
You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.
What should you include in the response plan?

A. controlled folder access
B. application isolation
C. memory scanning
D. machine isolation
E. user isolation

Answer: D

NEW QUESTION 127
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.
You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

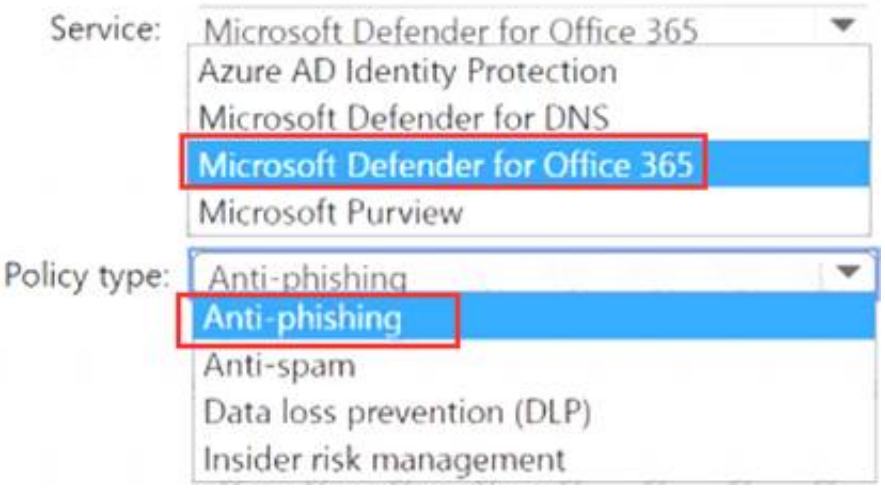
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 131
- (Exam Topic 3)
A customer has a Microsoft 365 E5 subscription and an Azure subscription.
The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.
You need to recommend a solution for the customer. The solution must minimize costs. What should you include in the recommendation?

A. Microsoft 365 Defender
B. Microsoft Defender for Cloud
C. Microsoft Defender for Cloud Apps
D. Microsoft Sentinel

Answer: D

NEW QUESTION 133
- (Exam Topic 3)
Your company plans to provision blob storage by using an Azure Storage account The blob storage will be accessible from 20 application sewers on the internet.
You need to recommend a solution to ensure that only the application servers can access the storage account. What should you recommend using to secure the blob storage?

A. service tags in network security groups (NSGs)
B. managed rule sets in Azure Web Application Firewall (WAF) policies
C. inbound rules in network security groups (NSGs)
D. firewall rules for the storage account
E. inbound rules in Azure Firewall

Answer: D

NEW QUESTION 136
- (Exam Topic 3)
You design cloud-based software as a service (SaaS) solutions.
You need to recommend ransomware attacks. The solution must follow Microsoft Security Best Practices. What should you recommend doing first?

A. Implement data protection.
B. Develop a privileged access strategy.
C. Prepare a recovery plan.
D. Develop a privileged identity strategy.

Answer: C

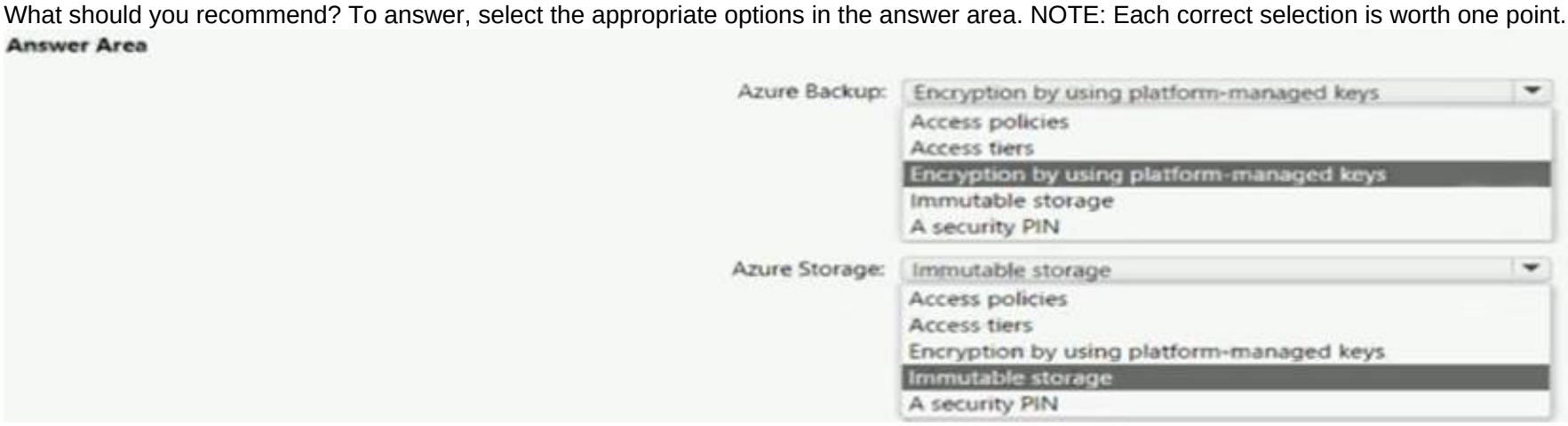
NEW QUESTION 139
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription.
You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

A. Microsoft Defender for Cloud Apps
B. insider risk management
C. Microsoft Information Protection
D. Azure Purview

Answer: C

Explanation:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide
You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as SalesForce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.

NEW QUESTION 142
- (Exam Topic 3)
Your company wants to optimize using Azure to protect its resources from ransomware.
You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 146
- (Exam Topic 3)
Your company uses Azure Pipelines and Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows for the deployment of applications to Azure.
You are updating the deployment process to align with DevSecOps controls guidance in the Microsoft Cloud Adoption Framework for Azure.
You need to recommend a solution to ensure that all code changes are submitted by using pull requests before being deployed by the CI/CD workflow.
What should you include in the recommendation?

A. custom roles in Azure Pipelines
B. branch policies in Azure Repos
C. Azure policies
D. custom Azure roles

Answer: B

NEW QUESTION 147
- (Exam Topic 3)
You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender
You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender
You need to recommend a solution to meet the following requirements:
• Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
• Automatically generate incidents when the IP address of a command-and control server is detected in the events
What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

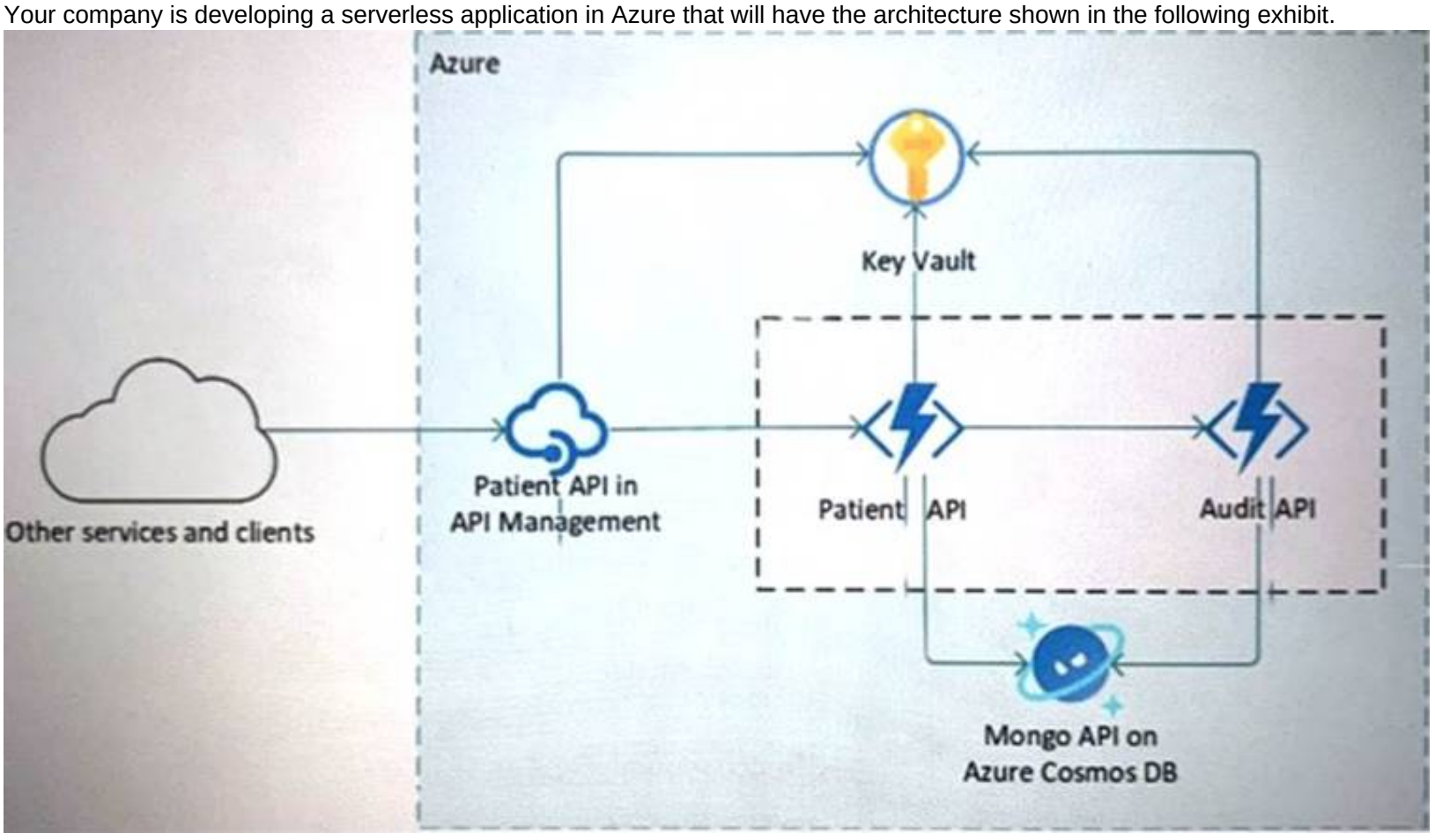
NEW QUESTION 151
- (Exam Topic 3)
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect f personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG)
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
• Ensure that each time the support staff connects to a jump server; they must request access to the server.
• Ensure that only authorized support staff can initiate SSH connections to the jump servers.
• Maximize protection against brute-force attacks from internal networks and the internet.
• Ensure that users can only connect to the jump servers from the internet.
• Minimize administrative effort
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 153
- (Exam Topic 3)
Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.



You need to recommend a solution to isolate the compute components on an Azure virtual network. What should you include in the recommendation?

A. Azure Active Directory (Azure AD) enterprise applications
B. an Azure App Service Environment (ASE)
C. Azure service endpoints
D. an Azure Active Directory (Azure AD) application proxy

Answer: B

Explanation:
App Service environments (ASEs) are appropriate for application workloads that require:
Very high scale,Isolation and secure network access,High memory utilization.This capability can host your: Windows web apps,Linux web apps Docker containers,Mobile apps Functions
https://docs.microsoft.com/en-us/azure/app-service/environment/overview

NEW QUESTION 156
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.
The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.
You have remote users who have personal devices that run Windows 11.
You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:
• Prevent the remote users from accessing any other resources on the network.
• Support Azure Active Directory (Azure AD) Conditional Access.
• Simplify the end-user experience.
What should you include in the recommendation?

A. Azure AD Application Proxy
B. Azure Virtual WAN
C. Microsoft Tunnel
D. web content filtering in Microsoft Defender for Endpoint

Answer: A

Explanation:
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

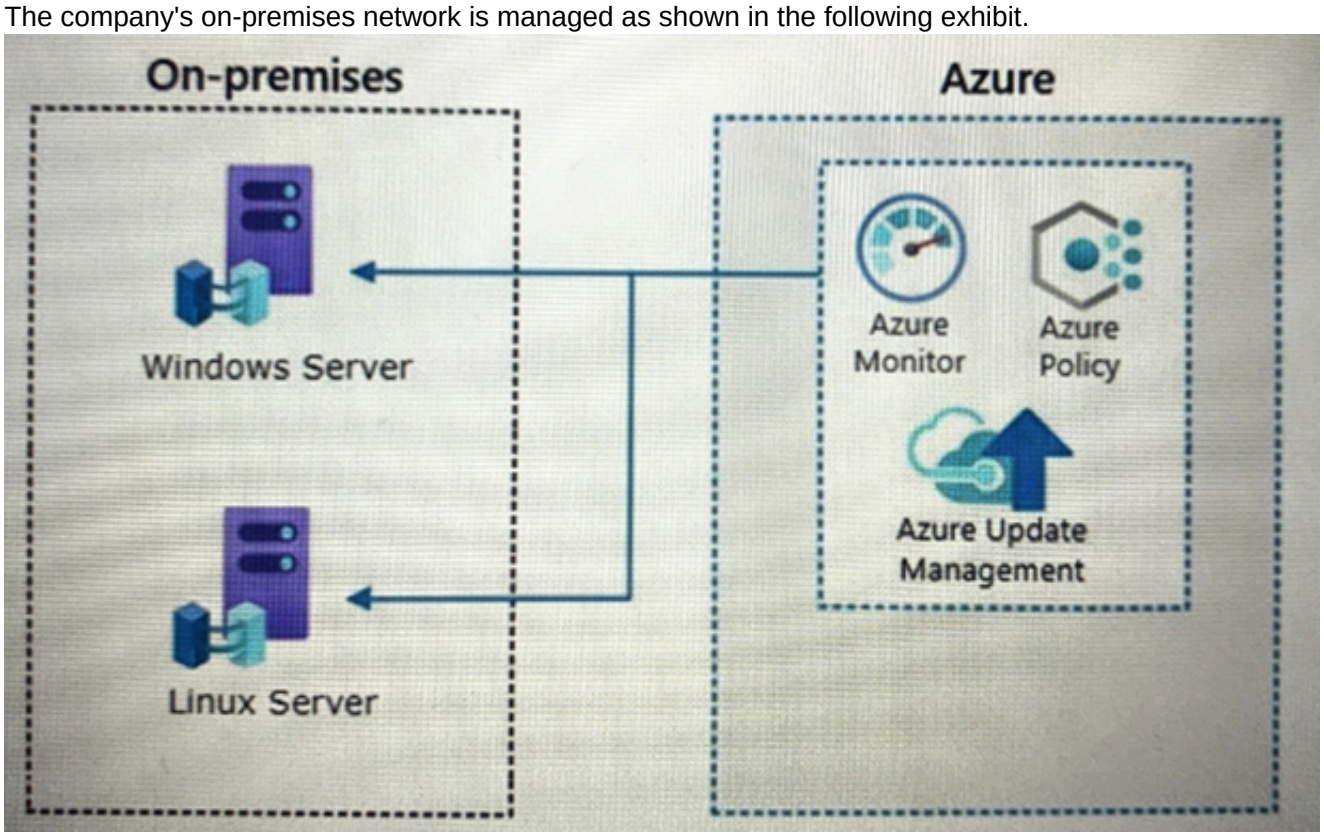
NEW QUESTION 157
- (Exam Topic 3)

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.
You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 161
- (Exam Topic 3)
Your company has a hybrid cloud infrastructure.
Data and applications are moved regularly between cloud environments.
The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:
- Govern virtual machines and servers across multiple environments.
- Enforce standards for all the resources across all the environment across the Azure policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.
NOTE Each correct selection is worth one point.

A. Azure VPN Gateway
B. guest configuration in Azure Policy
C. on-premises data gateway
D. Azure Bastion
E. Azure Arc

Answer: BE

Explanation:
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

NEW QUESTION 165
- (Exam Topic 3)
Your company has a Microsoft 365 E5 subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:
• Identify unused personal data and empower users to make smart data handling decisions.
• Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
• Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

A. Microsoft Viva Insights
B. Advanced eDiscovery
C. Privacy Risk Management in Microsoft Priva
D. communication compliance in insider risk management

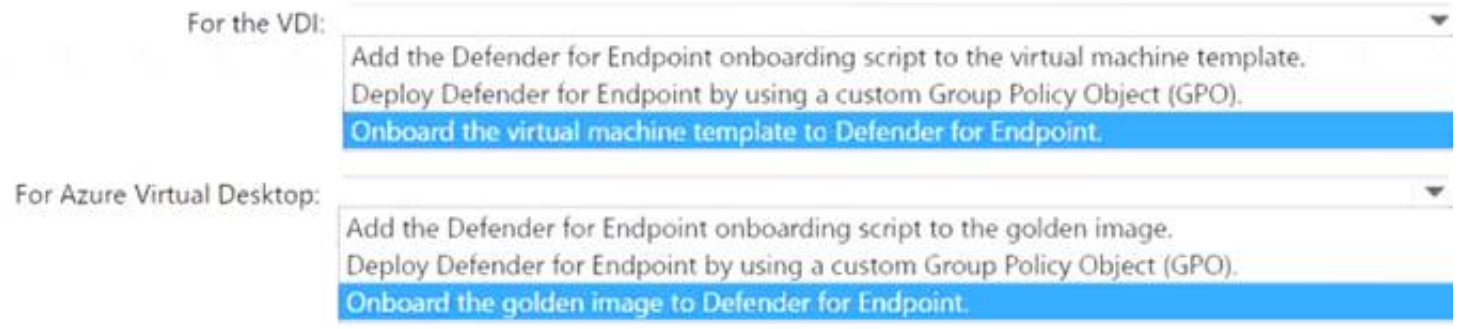
Answer: C

Explanation:
Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you:Detect overexposed personal data so that users can secure it.Spot and limit transfers of personal data across departments or regional borders.Help users identify and reduce the amount of unused personal data that you store.
https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management

NEW QUESTION 166

- (Exam Topic 3)
You have an Active Directory Domain Services (AD DS) domain that contains a virtual desktop infrastructure (VDI). The VDI uses non-persistent images and cloned virtual machine templates. VDI devices are members of the domain.
You have an Azure subscription that contains an Azure Virtual Desktop environment. The environment contains host pools that use a custom golden image. All the Azure Virtual Desktop deployments are members of a single Azure Active Directory Domain Services (Azure AD DS) domain.
You need to recommend a solution to deploy Microsoft Defender for Endpoint to the hosts. The solution must meet the following requirements:
• Ensure that the hosts are onboarded to Defender for Endpoint during the first startup sequence.
• Ensure that the Microsoft Defender 365 portal contains a single entry for each deployed VDI host.
• Minimize administrative effort.
What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

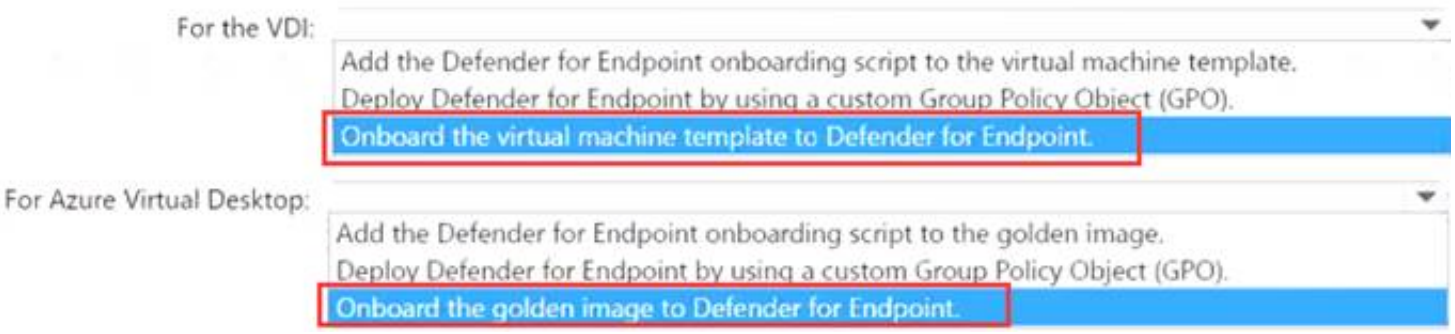


A. Mastered
B. Not Mastered

Answer: A

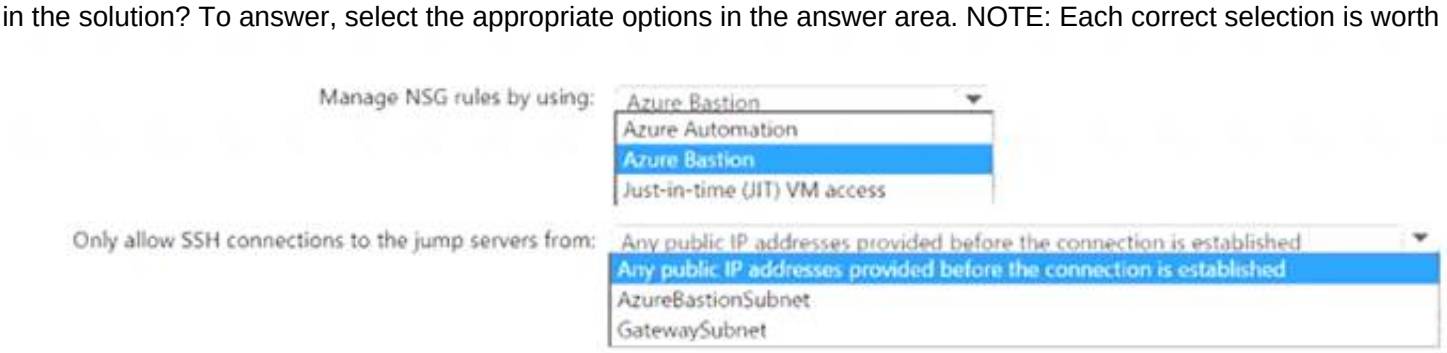
Explanation:

Answer Area



NEW QUESTION 169
- (Exam Topic 3)
You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG).
You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:
• Ensure that each time the support staff connects to a jump server; they must request access to the server.
• Ensure that only authorized support staff can initiate SSH connections to the jump servers.
• Maximize protection against brute-force attacks from internal networks and the internet.
• Ensure that users can only connect to the jump servers from the internet.
• Minimize administrative effort.
What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 173
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are designing the encryption standards for data at rest for an Azure resource.
You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.
Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses Microsoft-managed keys.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 174
- (Exam Topic 3)
Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities.
You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

A. standalone sensors
B. honeytoken entity tags
C. sensitivity labels
D. custom user tags

Answer: B

Explanation:
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

NEW QUESTION 177
- (Exam Topic 3)
Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud.
The company signs a contract with the United States government.
You need to review the current subscription for NIST 800-53 compliance. What should you do first?

A. From Defender for Cloud, review the secure score recommendations.
B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.
C. From Defender for Cloud, review the Azure security baseline for audit report.
D. From Defender for Cloud, add a regulatory compliance standard.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula

NEW QUESTION 182
- (Exam Topic 3)
You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux. You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:
• Identify missing updates and insecure configurations.
• Use the Qualys engine. What should you use?

A. Microsoft Defender for Servers
B. Microsoft Defender Threat Intelligence (Defender TI)
C. Microsoft Defender for Endpoint
D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: A

NEW QUESTION 185
- (Exam Topic 3)
Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines
You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines. What should recommend? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

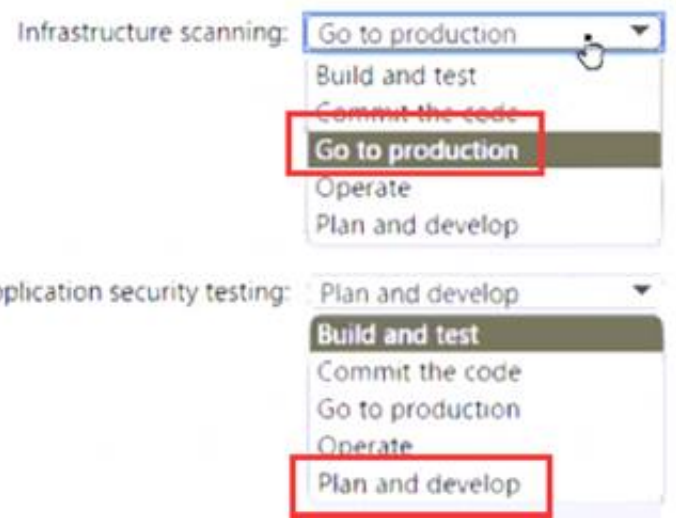
Answer Area

A. Mastered
B. Not Mastered

Answer: A

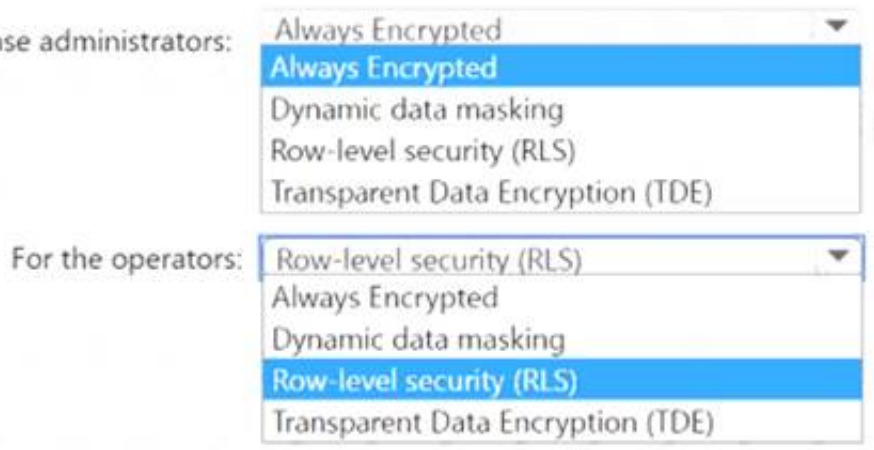
Explanation:

Answer Area



NEW QUESTION 189
- (Exam Topic 3)
You have an Azure SQL database named DB1 that contains customer information. A team of database administrators has full access to DB1.
To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information.
You need to design a security strategy for D81. The solution must meet the following requirements:
• When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.
• When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.
What should you include in the design? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

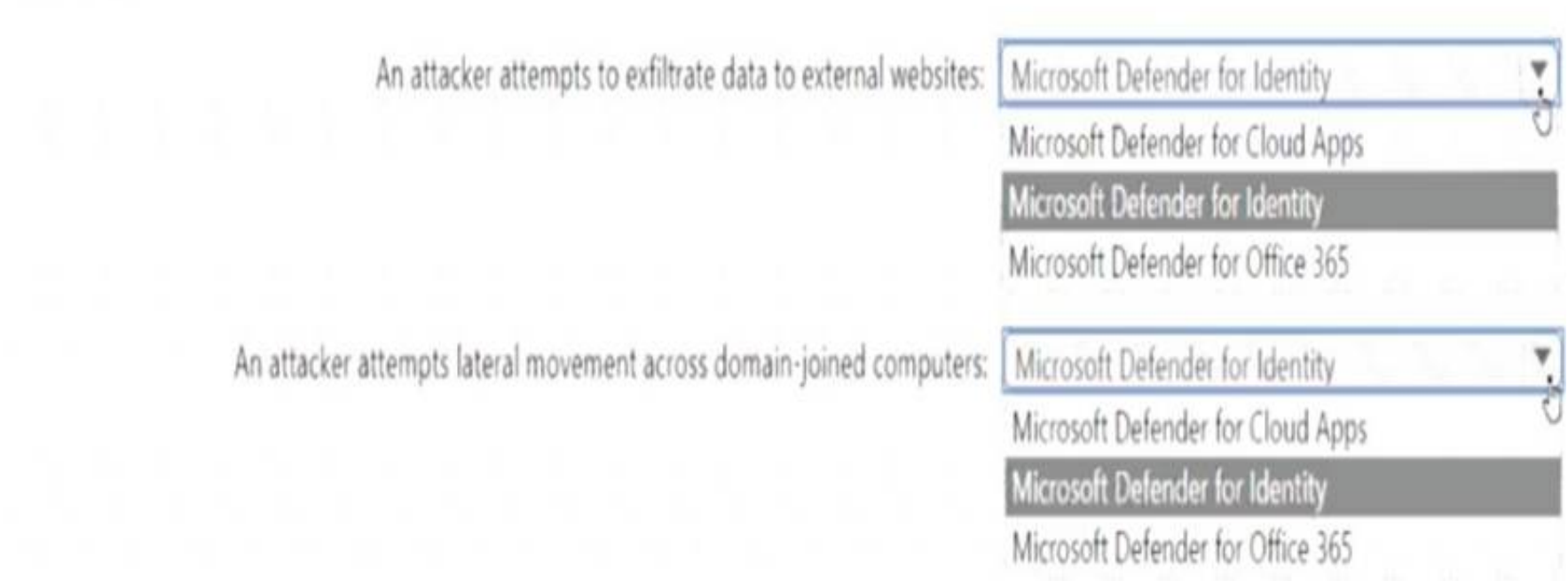


A. Mastered
B. Not Mastered

Answer: A

Explanation:

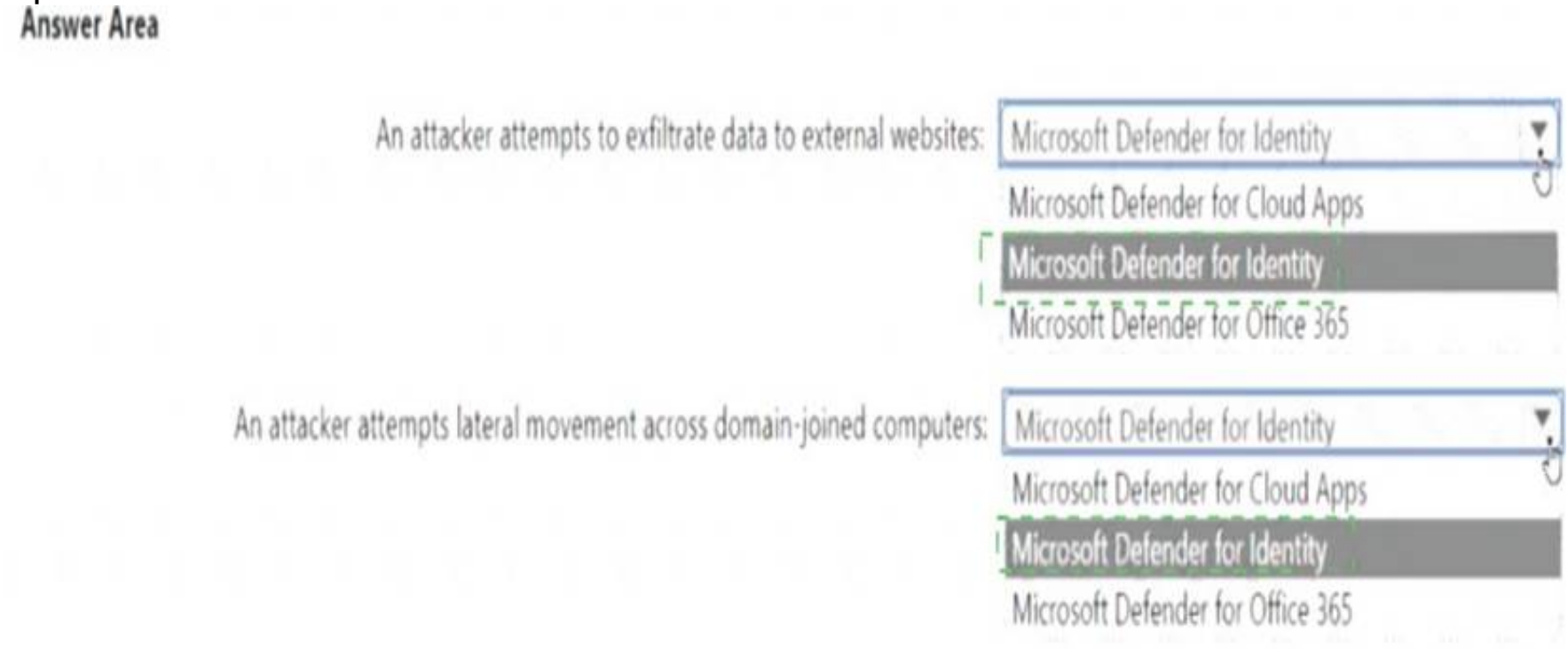
NEW QUESTION 190
- (Exam Topic 3)
For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA). You need to protect against the following external threats of an attack chain:
• An attacker attempts to exfiltrate data to external websites.
• An attacker attempts lateral movement across domain-joined computers.
What should you include in the recommendation for each threat? To answer, select the appropriate options in the answer area.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 194
- (Exam Topic 3)
Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/bastion/vnet-peering
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

NEW QUESTION 199
- (Exam Topic 3)
You plan to automate the development and deployment of a Nodejs-based app by using GitHub. You need to recommend a DevSecOps solution for the app. The solution must meet the following
requirements:
• Automate the generation of pull requests that remediate identified vulnerabilities.
• Automate vulnerability code scanning for public and private repositories.
• Minimize administrative effort.
• Minimize costs.
What should you recommend using? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
A close up of a text Description automatically generated

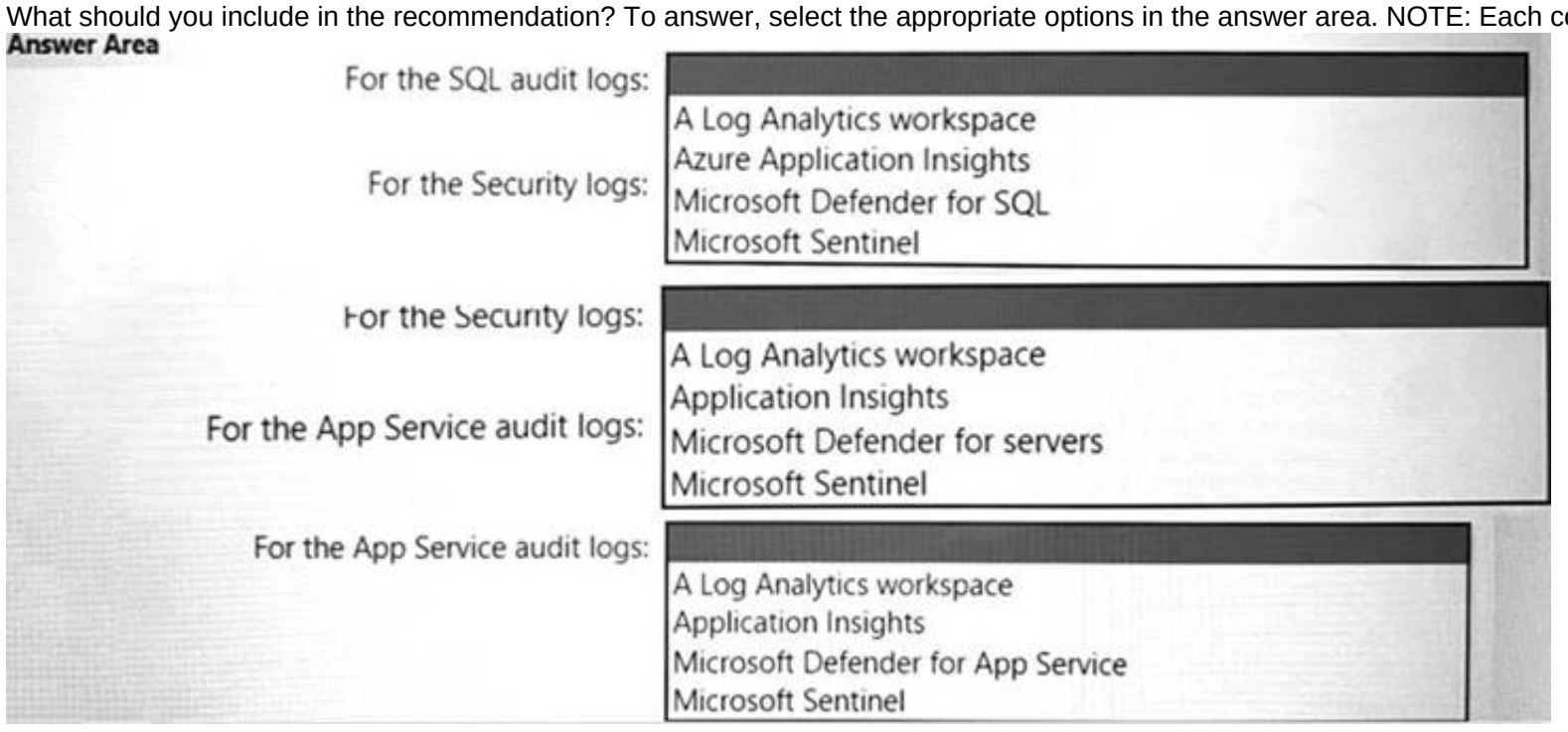
NEW QUESTION 204
- (Exam Topic 3)
You have an Azure subscription. The subscription contains 100 virtual machines that run Windows Server. The virtual machines are managed by using Azure Policy and Microsoft Defender for Servers.
You need to enhance security on the virtual machines. The solution must meet the following requirements:
• Ensure that only apps on an allowlist can be run.
• Require administrators to confirm each app added to the allowlist.
• Automatically add unauthorized apps to a blocklist when an attempt is made to launch the app.
• Require administrators to approve an app before the app can be moved from the blocklist to the allowlist. What should you include in the solution?

A. a compute policy in Azure Policy
B. admin consent settings for enterprise applications in Azure AD
C. adaptive application controls in Defender for Servers
D. app governance in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 208
- (Exam Topic 3)
You are designing an auditing solution for Azure landing zones that will contain the following components:
• SQL audit logs for Azure SQL databases
• Windows Security logs from Azure virtual machines
• Azure App Service audit logs from App Service web apps
You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:
• Log all privileged access.

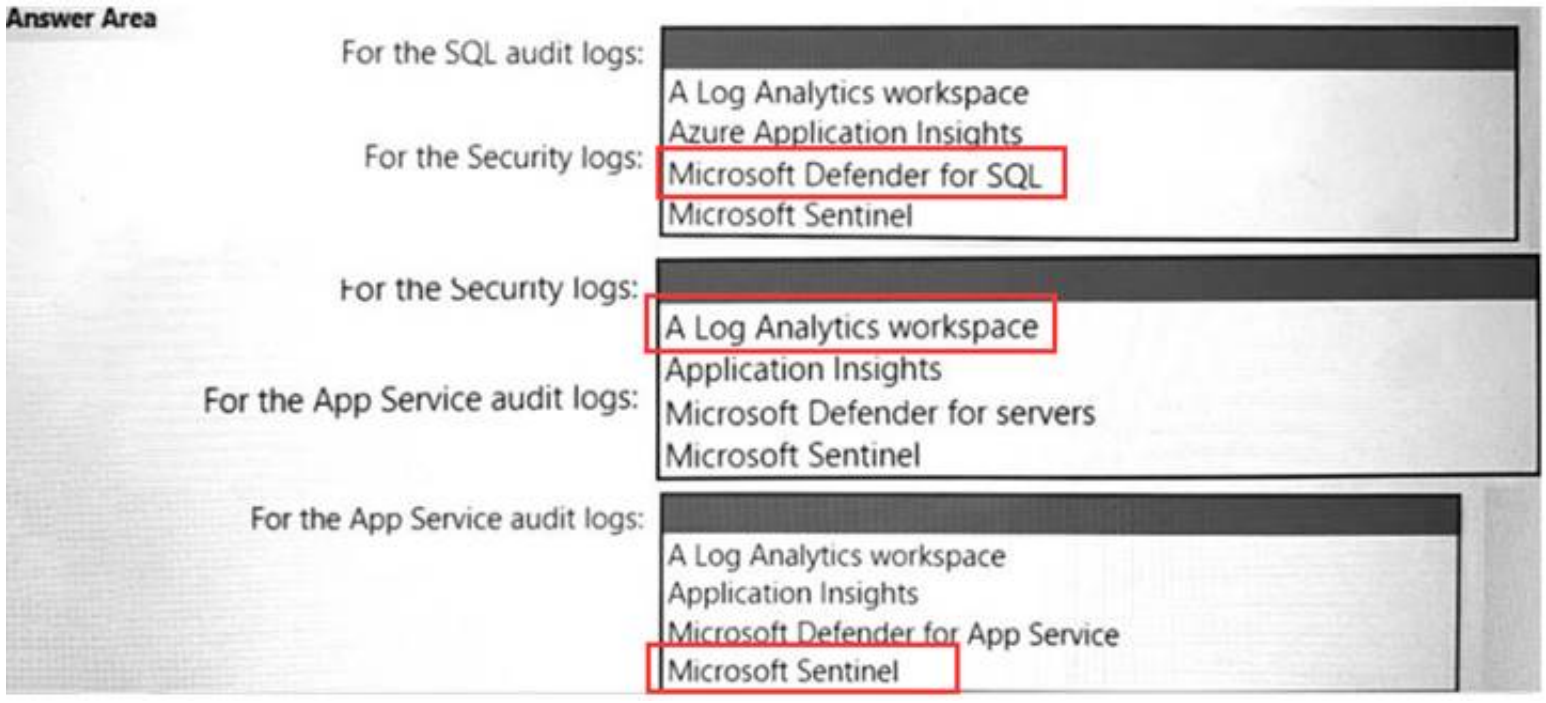
• Retain logs for at least 365 days.
• Minimize costs.
What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



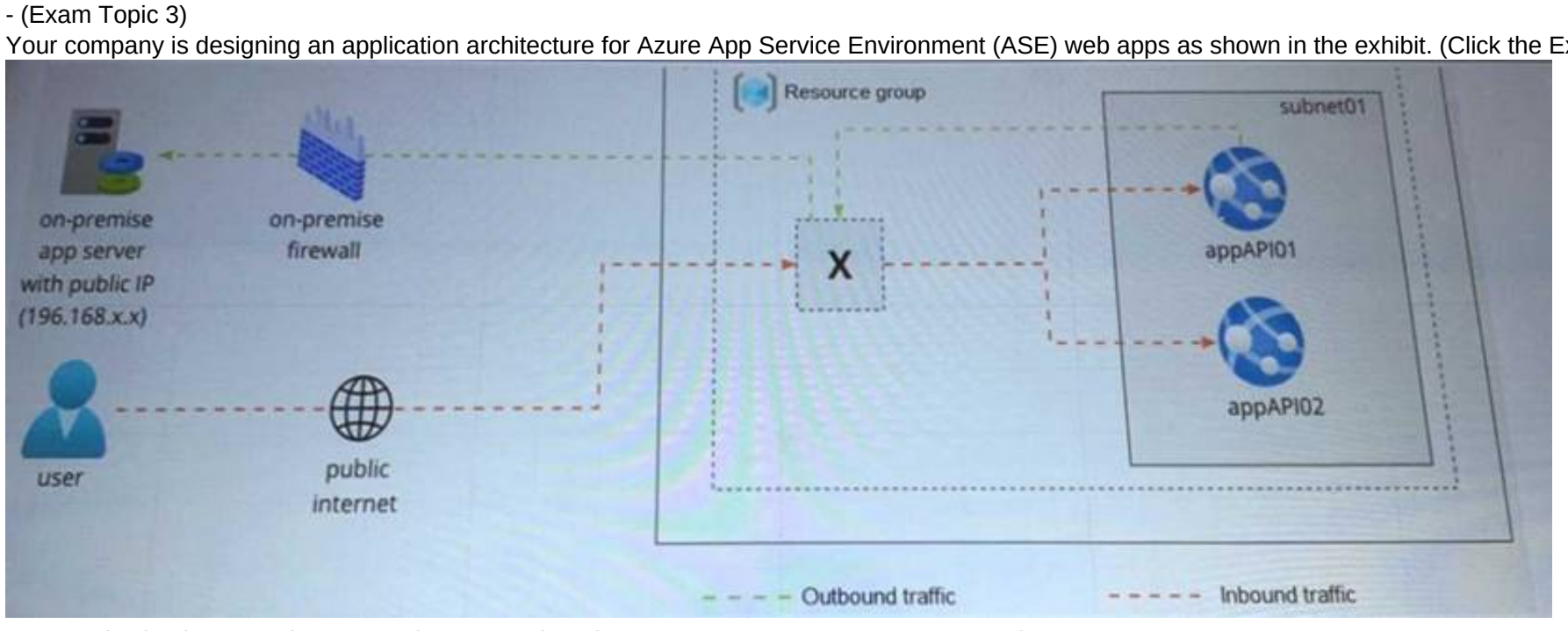
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 209
- (Exam Topic 3)
Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.
You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.
What should you include in the recommendation?

A. Azure Traffic Manager with priority traffic-routing methods
B. Azure Application Gateway v2 with user-defined routes (UDRs).

C. Azure Front Door with Azure Web Application Firewall (WAF)
D. Azure Firewall with policy rule sets

Answer: C

Explanation:
https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

NEW QUESTION 213
- (Exam Topic 3)
You have 50 Azure subscriptions.
You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.
NOTE: Each correct selection is worth one point.

A. Assign an initiative to a management group.
B. Assign a policy to each subscription.
C. Assign a policy to a management group.
D. Assign an initiative to each subscription.
E. Assign a blueprint to each subscription.
F. Assign a blueprint to a management group.

Answer: AF

Explanation:
https://docs.microsoft.com/en-us/azure/governance/management-groups/overview https://docs.microsoft.com/en-us/azure/governance/blueprints/overview https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001 https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

NEW QUESTION 214
- (Exam Topic 3)
You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance. You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.
Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend

NEW QUESTION 218
- (Exam Topic 3)
You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.
All resources are backed up multiple times a day by using Azure Backup. You are developing a strategy to protect against ransomware attacks.
You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.
Which two controls should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Use Azure Monitor notifications when backup configurations change.
B. Require PINs for critical operations.
C. Perform offline backups to Azure Data Box.
D. Encrypt backups by using customer-managed keys (CMKs).
E. Enable soft delete for backups.

Answer: AB

Explanation:
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware 'You need to recommend which CONTROLS must be enabled to ENSURE that Azure Backup can be used to RESTORE the resources in the event of a successful ransomware attack.' Whilst helpful for auditing purposes and detection of a malicious attack, monitoring configuration changes and alerting after a change is made does not represent a CONTROL which ENSURES Azure Backup can be used to RESTORE the resources.

NEW QUESTION 222
- (Exam Topic 3)
You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.
You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.
What should you include in the recommendation?

A. Apply read-only locks on the storage accounts.
B. Set the AllowSharcdKeyAccess property to false.
C. Set the AllowBlobPublicAcccss property to false.
D. Configure automated key rotation.

Answer: A

Explanation:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

NEW QUESTION 227
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SC-100 Practice Exam Features:

* SC-100 Questions and Answers Updated Frequently

* SC-100 Practice Questions Verified by Expert Senior Certified Staff

* SC-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year